Marguerite BRAC DE LA PERRIERE*

Règlement général européen sur la protection des données (RGPD) à caractère personnel
Partie 1 : Origine, objectifs et implications

RÉSUMÉ

Le règlement général sur la protection des données (RGPD), entré en vigueur le 27 avril 2016, sera applicable le 25 mai 2018. Ce nouveau règlement s'inscrit dans la droite lignée de la Loi informatique et libertés du 6 janvier 1978. Il constitue une évolution de la réglementation relative à la protection des données personnelles dont les principes fondateurs ont été réaffirmés, voire, précisés ou rebaptisés. Cet article propose une revue succincte de l'origine, des objectifs et des implications de ce texte quel que soit le cadre sectoriel d'application.

MOTS-CLÉS

Règlement général européen sur la protection des données (RGPD) - Responsabilité - CNIL

European General Regulation on Data Protection (GDPR)

Part 1: Origin, objectives and implications

SUMMARY

The General Data Protection Regulation (GDPR), which came into effect on April 27, 2016, will be applicable on May 25, 2018. This new regulation is in line with the French law "Informatique et libertés" of January 6, 1978. It constitutes an evolution of the regulations on the protection of personal data whose founding principles have been reaffirmed, even specified or renamed. This article provides a brief review of the origin, objectives and implications of this text, regardless of the sectoral application framework.

KEYWORDS

General Data Protection Regulation (GDPR) - Accountability - Data Protection Authority (DPA)

I - Origine du RGPD

Le règlement général sur la protection des données (1) (RGPD), entré en vigueur le 27 avril 2016, sera applicable le 25 mai 2018.

Ce nouveau règlement s'inscrit dans la droite lignée et le respect de la Loi informatique et libertés du 6 janvier 1978 (2) modifiée en 2004 afin de transposer en droit interne la Directive européenne de 1995 (3). En effet, il constitue une évolution - mais en aucun cas une révolution - de la réglementation relative à la protection des données personnelles dont les principes fondateurs ont été réaffirmés, voire, le cas échéant, précisés ou rebaptisés :

(i) les données à caractère personnel doivent être traitées de manière **licite, loyale et transparente** au regard de la personne concernée ;

(ii) les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités, dans le respect du principe de **limitation des finalités** ;

(iii) les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées, dans le respect du principe de **minimisation des données** ;

(iv) les données doivent être exactes, et si nécessaires tenues à jour, dans le respect du principe d'**exactitude** ;

(v) les données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités, dans le respect du principe de **limitation de la conservation** ;

(vi) les données doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques et organisationnelle appropriées, aux fins du respect de leur **intégrité** et **confidentialité**.

* Avocate, directrice du département santé numérique, Lexing Alain Bensoussan Avocats – 58 Boulevard Gouvion-Saint-Cyr – 75017 Paris
Tél. : +33 (0)1 82 73 05 05 – www.alain-bensoussan.com

II - Objectifs

Le RGPD a pour vocation générale, tenant compte de l'évolution rapide des technologies, d'offrir un cadre de la protection des données à caractère personnel plus solide et cohérent dans l'Union, et de l'assortir d'une application rigoureuse des règles afin de susciter la confiance des individus et le développement de l'économie numérique.

De manière plus spécifique, le RGPD poursuit en particulier trois principaux objectifs :
placer les personnes concernées au cœur des traitements des données, responsabiliser les responsables de traitement, et enfin crédibiliser les autorités.

1. Placer les personnes concernées au cœur des traitements des données

Afin d'atteindre le premier des principaux objectifs du RGPD, il faut :

(i) au moment de la collecte des données ou, en cas de collecte indirecte, dans un délai raisonnable en fonction des circonstances propres à chaque cas, assurer une **information plus complète, accessible, compréhensible,** des personnes concernées sur les caractéristiques des traitements de leurs données - à commencer par la ou les finalités - mais aussi sur les risques, règles, garanties et droits liés au traitement, et modalités d'exercice de leurs droits ;
(ii) **renforcer les droits des personnes concernées**, en facilitant leur exercice, en leur offrant de nouveaux droits tels que les droits à la portabilité, à la limitation, à l'oubli, et en assurant des réponses plus rapides de la part des responsables de traitement ;
(iii) donner un **rôle plus central au consentement de la personne concernée.**

2. Responsabiliser les responsables de traitement

Responsabiliser les responsables de traitement, pour répondre au deuxième objectif principal du RGPD, implique de sortir de la logique de formalités préalables, et de mettre à la charge de ces responsables de nouvelles obligations. Leur mise en œuvre résultera notamment de l'utilisation de nouveaux moyens et outils tels que le délégué à la protection des données (DPD, ou DPO pour *data protection officer*, en anglais), le registre des traitements, ou l'analyse d'impact.

3. Crédibiliser les autorités

Le troisième objectif principal du RGDP est de crédibiliser les autorités :
(i) en assurant une **coopération entre Cnil européennes** notamment au moyen du mécanisme de guichet unique, pour que chaque responsable de traitements conduits au sein de plusieurs états membres, puisse s'adresser à une seule autorité de contrôle chef de file ;
(ii) en renforçant leur **pouvoir de sanctions dissuasives** des infractions à la réglementation, sanctions qui peuvent désormais s'élever à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, ou 20 millions d'euros, le montant le plus élevé étant retenu.

III - Implications

Le RGPD porte en germe près de 400 obligations dont le contenu est précisé dans 99 articles, contextualisés par 173 considérants.

Chaque responsable de traitement doit désormais réfléchir « protection des données » tant au moment de la détermination des moyens de traitement (dès la conception), qu'au moment du traitement lui-même. Il doit s'assurer que, par défaut, les données sont gérées avec le niveau de sécurité physique et logique approprié au traitement, et être en mesure, à tout moment, de documenter les mesures prises (mécanismes et procédures internes) afin de respecter les exigences du RGPD en matière de responsabilité (« *accountability* »).

Le compte à rebours est donc largement entamé avant l'applicabilité, le 25 mai 2018, du RGPD. En effet, pour être en conformité, chaque responsable de traitement et chaque sous-traitant doit avoir préalablement :

(i) cartographié les traitements de données à caractère personnel qu'il réalise, et leurs caractéristiques,
(ii) aux fins de mettre en exergue les écarts entre celles-ci et les exigences du RGPD, et ce
(iii) pour identifier les actions à entreprendre, et y assortir un calendrier ;
(iv) pour, enfin, commencer à déployer les actions de mise en conformité.

Par ailleurs, le RGPD renvoie à un état de l'art sectoriel aux fins de déterminer les mesures à prendre pour garantir la sécurité d'un traitement en particulier.
En effet, le RGPD impose aux responsables de traitements, et sous-traitants, de mettre en œuvre les mesures techniques et organisationnelles **appropriées** afin de garantir un niveau de sécurité adapté au risque, et ce, compte tenu de l'état des connaissances, des coûts de mise en œuvre, et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les personnes physiques.

Ainsi, s'agissant du secteur de la santé, les mesures techniques et organisationnelles appropriées à mettre en œuvre relèvent :

(i) de nombreux référentiels sectoriels tels que la PGSSI-S (4), le référentiel sur l'hébergement de données de santé ;
(ii) de recommandations issues de délibérations de la Cnil ;
(iii) de bonnes pratiques résultant de la doctrine d'autorités sectorielles telles que l'ASIP Santé ou les Conseils Nationaux de l'Ordre des Médecins ou des Pharmaciens, outre celles des autorités non sectorielles telle que l'ANSSI (Agence nationale de la sécurité des systèmes d'information) ;
(iv) et enfin, de textes normatifs spécifiquement applicables.

Dans ce contexte où l'identification des mesures à prendre pour se mettre en conformité peut s'avérer particulièrement ardue, c'est naturellement que sont encouragées :

(i) l'élaboration de codes de conduites sectoriels, dont le respect « *peut servir d'élément pour démontrer le respect des obligations incombant au responsable de traitement* » ;
(ii) la mise en place de mécanismes de certification et de labels, « *aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le [...] règlement* ».

RÉFÉRENCES

(1) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), Journal officiel de l'Union européenne, 4 mai 2016, disponible à http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679

(2) Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée

(3) Directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Journal officiel de l'Union européenne, 24 octobre 1995, disponible à http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:31995L0046

(4) PGSSI-S, Politique générale de sécurité des systèmes d'information de santé, 1e octobre 2015, disponible à http://esante.gouv.fr/services/politique-generale-de-securite-des-systemes-d-information-de-sante-pgssi-s/en-savoir-plus-0